In re Application of: Eli YANOVSKY
Serial No.: 10/520,274
Filed: January 18, 2005
Office Action Mailing Date: June 8, 2010

Examiner: KANAAN Simon P.
Group Art Unit: 2432
Attorney Docket: 29238

REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1 - 48 are in this Application. Claims 1 – 48 have been rejected under 35 U.S.C. § 103. Claim 21 has been amended herewith.

35 U.S.C. § 102 Rejections

Claims 1, 2, 19, 21 and 37 have been rejected for lack of novelty over Atalla.

Claims 1, 21 and 37 were amended in the previous responses to stress the point that the *encryption keys* are *generated separately* at the two different parties, using separate randomizers, which have identical settings.

Beginning with claim 1, the claim requires inter alia:

> "a datastream extractor, configured to *extract a bitstream* from data exchanged between said parties;
>
> a random selector configured with selection settings identical to those at said second party said selection settings *defining a selection, from said bitstream*, of a series of bits in accordance with a randomization within said random selector, *said randomization seeded by said data exchanged between said parties*, said randomization being identical to a randomization carried out at said second party, thereby ensuring that said series of bits is identically selected at both parties;".

Atalla Fig. 7 does not show *extraction of a bitstream from* data exchanged between the parties. Neither does it show the claimed step of *making a selection from the bitstream of a series of bits*, and it certainly does not show *a randomization seeded by the data exchanged is used to make that selection.*

That is to say claim 1 defines a number of distinct stages that are carried out with the data exchanged between the parties.

Atalla in stark contrast, describes Fig. 7 between column 9 line 65 and column 10 line 44. The two computers transmit addresses which are then used to obtain data from a session key held at each party. There is no further operation on the data exchanged between the parties, certainly not the three-element process defined in claim 1.

Claim 37 as currently drafted also requires such a three-stage operation with the data exchanged. Specifically, claim 37 requires:

> "sharing with said remote party a primary data stream,
>
> using said primary data stream and identical settings at each party to form an identical randomizer at each party,
>
> selecting parts of said primary data stream using said identical randomizer at each party to form identical derived data sources independently at each party,".

Atalla indeed shares the addresses between the parties. However once he has done this there is no more random selection of data exchanged between the parties. Thus he certainly fails to teach the third step of selecting *parts of the primary data stream using the identical randomizer* at each party. Rather as taught in the description of Fig. 7 of Atalla, once the addresses are exchanged they are applied to the original keys held at the parties separately, which are never exchanged.

Claim 21 teaches:

> "a selector configured with identical settings, said settings *defining a random selection* at predetermined selection intervals, *of parts of said primary bitstream* to form *a derived bit source*, each selector being operable to *use said derived bit source,* in an identical manner, *to randomize said selecting from said primary bitstream*, said identical settings ensuring that each party derives an identical derived bit source,".

That is to say, claim 21 also requires a derived selection to be made of data in the bitstream exchanged between the parties. In Atalla it is true that data exchanged between the parties is used to make a selection, but the selection is of data *already*

stored at the parties. There is no *derived* selection *of data exchanged between the parties* based on *primary random selection* of *data exchanged* between the parties.

Considering the case in more detail, US5,960,086 by Martin M. Atalla**,** teaches creating the same encryption key at both conversing parties, to encrypt a communication between them, by using a fixed long term **secret** master stored key of plurality of bytes, -- which **both parties hold and have beforehand;** for the creation of the encryption key. Addresses of bytes – meaning addresses of the bytes in that storage of a plurality of bytes - are sent in the open over insecure lines from one party to the other; then both parties select the same bytes from that same plurality of bytes to use to create the same encryption key. See Atalla's abstract: "Secure transmission of a message is achieved by using a one-time encryption key derived at the receiver and the sender from information present at both the sender and the receiver, but wherein the information from which the encryption key is derived *is not transmitted* between the sender and the receiver".

Reference is also made in this respect to Atalla page 3 lines 3 – 45 which make the point that the information from which the encryption key is derived is not transmitted between the sender and the receiver.

Thus the security of Atalla's system is guaranteed by the secrecy of the plurality of bytes that both parties hold for a long period of time. The addresses of bytes that are sent from one party to the other in the open over the insecure line are considered not to be enough information to break the system's security as long as the master storage of the plurality of bytes is kept in secret to any one other than the two conversing parties.

That is to say, Atalla teaches a long term master, a master secret mega storage of random bits. For each use the parties agree openly over the insecure line to addresses of bytes in that master. This is a long known technique, used long before Atalla, and to which we have already responded in earlier Office Actions.

But, once that fix long term master secret book is compromised, then the whole of Atalla's system is open to that third party. Compromising of the fixed long

term master secret book can be achieved by Phising, or by direct access to an organization's server, say through corruption.

In contrast to Atalla, the present application aims at overcoming this fault. A system is provided where random changes are based on fresh, and not fixed long-term, ongoing bit streams communicated between the conversing parties, to act as the changing random sources for the random processes to create the random changing encryption keys. All is done automatically between the conversing parties; and there are no such weak points to break the system.

The present invention teaches for the first time the possibility of two parties separately generating same random keys from information that is not in itself a partial keys or a master fixed long term secret storage of bytes, and which can be shared over an open link.

In view of the above amendments and remarks it is respectfully submitted that claims 1-48 are now in condition for allowance. A prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

/Jason H. Rosenblum/

Jason H. Rosenblum
Registration No. 56,437
Telephone: 718.246.8482

Date: December 1, 2010